REMARKS/ARGUMENTS

Claims 15-27 remain in this application.

The specification has been amended. No new matter has been added.

The Examiner has objected to the drawings. Amended drawings are enclosed to obviate this objection. Formal drawings will be provided when the application is allowed.

The Examiner has rejected the claims under 35 USC 112. Pursuant to the Examiner's comments, the claims have been amended to obviate this rejection. Antecedent support for the amendments to the claims that the second TCP/IP port is with the third node of the second network is found on page 8, lines 11-13.

The Examiner has rejected Claims 15-17 and 23-25 as being unpatentable over Keane. Applicant respectfully traverses this rejection.

Referring to Keane, there is disclosed methods and systems for firewalling virtual private networks. Keane teaches the installation and maintenance of a secure virtual private network over the Internet have been too complex, requiring financial investment in hardware, software, personnel, and/or time. A VPN solution that uses an enterprise-level firewall to protect against threats, such as hackers on the Internet may take up to a week to configure. In addition, certain users within a virtual private network may pose a security threat. For example, when an unscrupulous employee has access to certain portions of the virtual private network, he may attempt to access other portions of the network for which he is not authorized. See paragraph 18.

Keane teaches a network operations center 102 may form a virtual private network using a first encrypted information flow to exchange control information with the Gateway 106, and a second encrypted information flow to exchange control information with Gateway 108. Network operations center 102 may also enable a third encrypted information flow 126 between Gateways 106 and 108 for the virtual private network. See paragraph 38 and encrypted information flow, such as an encrypted tunnel, maybe established to base network 104 by encapsulating a protocol within another protocol. See paragraph 40.

Gateways 106 and 108 may provide an entrance and exit point for communications between these networks 104 and networks 110 and 112. See paragraph 44. Networks 110 and 112 may facilitate communication for a particular person, group, or enterprise. Tunnel interface module 202 of the network operations center establish tunnels between the network operations center 102 and Gateways 106, 108. Tunnel interface module 202 may include a public addressable or routable IP address that permits establishing tunnels, such as first and second encrypted flows, between network operations center 102 and gateways 106 and 108. Tunnel interface module 202 may include a transmission control protocol total driver used to establish a TCP tunnel between network operations center 102 and the gateways 106 108. The tunnel interface module may use the TCP tunnel driver to encapsulate packets for a tunnel within TCP packets. Alternatively, a tunnel interface module may use encryption and were tunnel software. See paragraph 51.

While encryption techniques may make communications private, authentication techniques may also allow communicating parties to verify each other's identity and the authenticity of the exchanged information. See paragraph 56. Firewalls 212 may include one or more processors, which may selectively limit the type of information reaching communication channel 216 and switch 214. For example, firewalls 212 may only permit entry of TCP commands to a specific port number. See paragraph 58.

A user may establish one or more rules that selectively restrict information flowing between base network 14, and networks 110 and 112. The user may specify which types of communications services of base network 104 are enabled, such as TCP or HTTP. The user may specify rules which route service requests for base network 100 for two specific processors and networks 110 and 112. See paragraph 62.

From the above description, it is clearly apparent that the use of a firewall, authentication techniques and rules are very different from applicants' claimed invention which requires a first TCP/IP port of a first node of a first network to communicate with a second TCP/IP port of a third node in a second network, where these TCP/IP ports have been predefined by an administrator and which remain constant and cannot be changed, as found in amended Claim 15. Furthermore, "the third node is only able to communicate with the first TCP/IP port of the first node via TCP/IP port extension using gatewayed methodology, such that the second node cannot be accessed by the third node" as found in Claim 15. It is respectfully submitted that Keane does not teach or suggest these limitations whatsoever and uses a completely different approach for security.

The Examiner recognizes that Keane does not expressly teach the first port is a TCP/IP port in the Office Action. The Examiner then goes on and says it would have been obvious to one of ordinary skill in the art at the time of the invention was made to have a first TCP/IP port in order to provide tunneling and encryption to their firewall solution. However, it is respectfully submitted that this entirely misses the point regarding applicant's claimed invention. Applicant does not rely on a firewall nor tunneling encryption in the claimed invention. As explained above, applicant's claimed invention utilizes a preset connection between two TCP/IP ports that is essentially permanent to limit the ability of an intruder to obtain unauthorized accesses. This does not rely on encryption, which may be broken, or rules, which may be circumvented, or authorization techniques, which could be bypassed, and which are specifically taught by Keane.

Accordingly, it is respectfully submitted that Keane does not teach or suggest any of the above-mentioned limitations of applicant's claimed invention, and Claims 15-17 and 23-25 are patentable.

The Examiner has rejected Claims 18-22, 26 and 27 has been unpatentable over Keane in view of Salama. Applicant respectfully traverses this rejection.

Referring to Salama, there is taught a method and apparatus for automatic inter domain routing of calls. Salama teaches a call is passed towards the destination address in regard to a call route of an IP telephony call. See column 8, lines 60-63. A review of Salama shows there is no concern, suggestion or even comment regarding the issue of security. Salama has nothing at all to do with secure communications. As its title suggests, Salama is only concerned with automatic inter-domain routing of calls. It is respectfully submitted that the teachings of Salama do not add anything, in relevant part, to the teachings of Keane, to arrive at independent Claims 15 and 23 of applicant.

Furthermore there must be some teaching or suggestion in the applied art or record to combine the teachings examiner is relying upon to arrive at applicant's claimed invention. It is respectfully submitted, there is no such teaching or suggestion. In fact, since Salama has nothing at all to do with security, there is absolutely no reason why one skilled in the art would look to Salama to arrive at applicant's claimed invention. Because Salama has nothing at all to do with security, it can be considered to be non-analogous art in regard to applicant's claimed invention. Accordingly, Claims 15 and 23 of applicant are patentable over the applied art or record. Claims 18-22, and 26 and 27 are dependent to parent Claims 15 and 23, respectively, and are patentable for the reasons Claims 15 and 23 are patentable.

In view of the foregoing amendments and remarks, it is respectfully requested that the outstanding rejections and objections to this application be reconsidered and withdrawn, and Claims 15-27, now in this application be allowed.

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

2/9/09
Date

Ansel M. Schwartz
Registration No. 30,587

Respectfully submitted,

Ansel M. Schwartz
Reg. No. 30,587
201 N. Craig Street, Suite 304
Pittsburgh, PA 15213
Tel.: (412) 621-9222